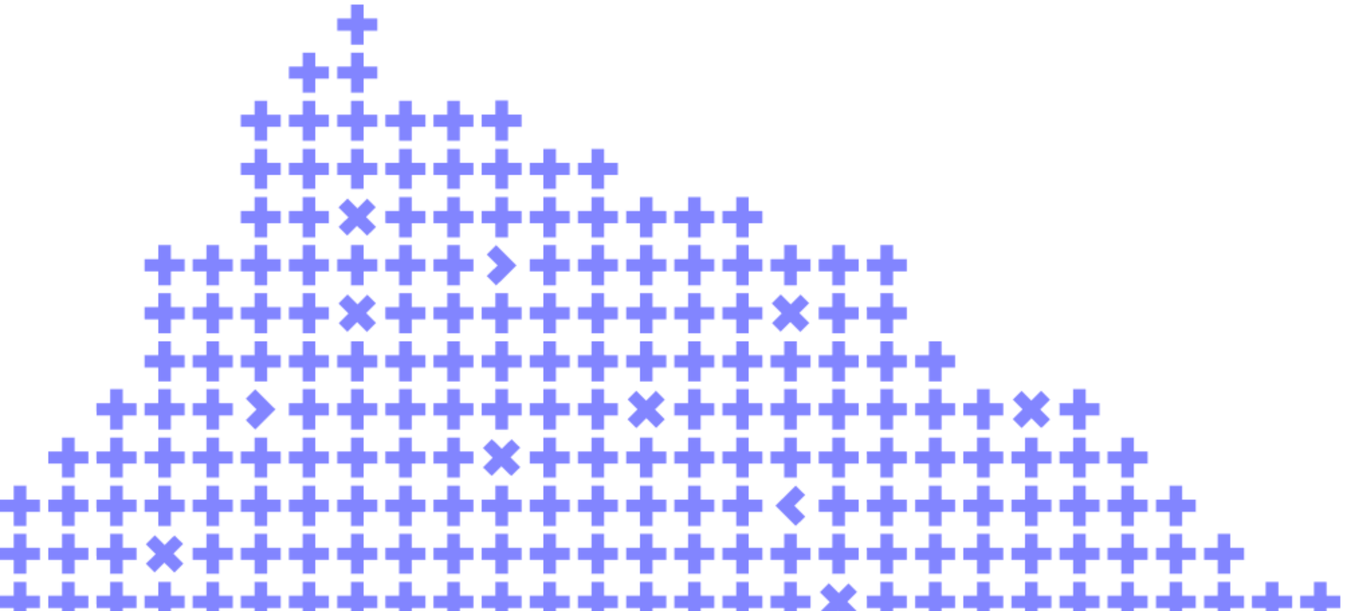
The clashes of the titans — Usability vs. Security. Can they live together?

Alon Kiriati



High Load ++ Armenia

Co-organizer

Yandex

Google

Are there available tickets for Scotland vs. Ukraine?

Scotland > Supporters & Tickets > Scotland Tickets

Hospitality | Membership | News | Newsletter

BUY SCOTLAND TICKETS

Keep up to date with the latest ticketing news via **Scotland National Team Twitter** and **Scotland National Team Facebook**.

Scotland v Ukraine

F.I.F.A. World Cup Play-off | A Squad

24/03/2022 7:45pm Glasgow

BUY ONLINE

Ticket Office

Buy Online

Scotland v Ukraine

F.I.F.A. World Cup Play-off | A Squad

24/03/2022 7:45pm Glasgow

BUY ONLINE

Tickets

MENS 'A' HOME GAMES

Find home tickets for upcoming Scotland Men's National Football Team.

BUY TICKETS

SCOTLAND MEN'S NATIONAL FOOTBALL TEAM

HOME MATCH PACKAGE 2022

Home Match Package 2022 Thursday, 24 March, 2022 - Friday, 23 September, 2022

CAN I BUY THIS PRODUCT?

You need to have purchased or have in your basket Scotland Supporters Club 2020-2021 *before buying this!*

IMPORTANT INFORMATION

*Package Includes - *FIFA World Cup Play Off - Scotland v Ukraine *UEFA Nations League - Scotland v Armenia *UEFA Nations League - Scotland v Ukraine *UEFA Nations League - Scotland v Republic of Ireland*

Select Seats

REGISTER NEW ACCOUNT

If you are a new customer who has never purchased tickets from The Scottish FA before, please click the 'Register New Account' button and register online now.

Register New Account

PERSONAL DETAILS (WHO THE MEMBERSHIP IS FOR)

Title*

--

Forename*

Surname*

Date of Birth*

-- -- --

Sex*

--

Email*

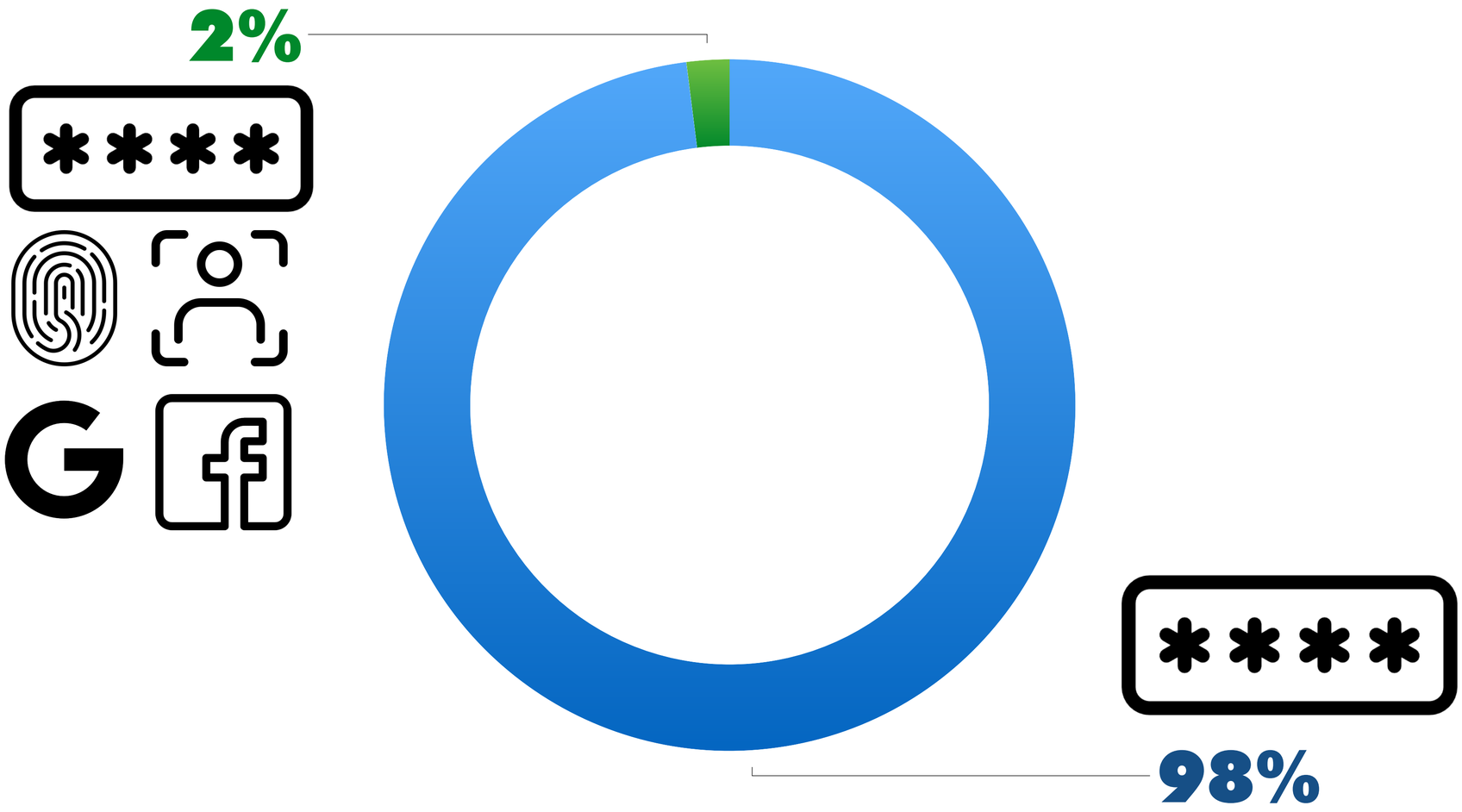
PASSWORD

(Passwords need be 8-64 characters long and contain 1 upper case letter, 3 lower case letters, 1 number and 1 special character e.g !@#£ %)

Password*

Confirm Password*

IS IT STILL 1990?



https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-password-is-slowly-becoming-extinct.aspx

DATA BREACHES

2.7B

$2.1T

https://en.wikipedia.org/wiki/List_of_data_breaches

IF IT HAPPENED TO THEM, IT CAN HAPPEN TO YOU

2020 / 200M users

2019 / 540M users

2019 / 250M users

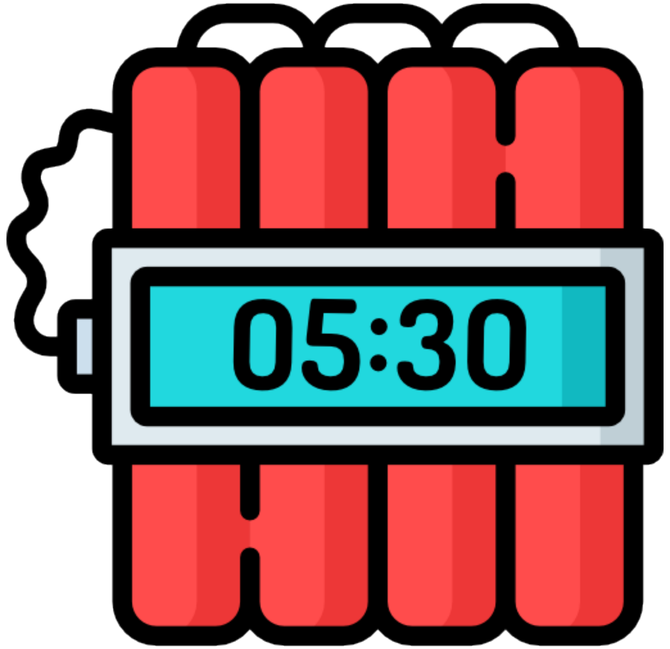
2017 / 57M users

2012 / 12M users

2013 / 4.7M users

https://en.wikipedia.org/wiki/List_of_data_breaches

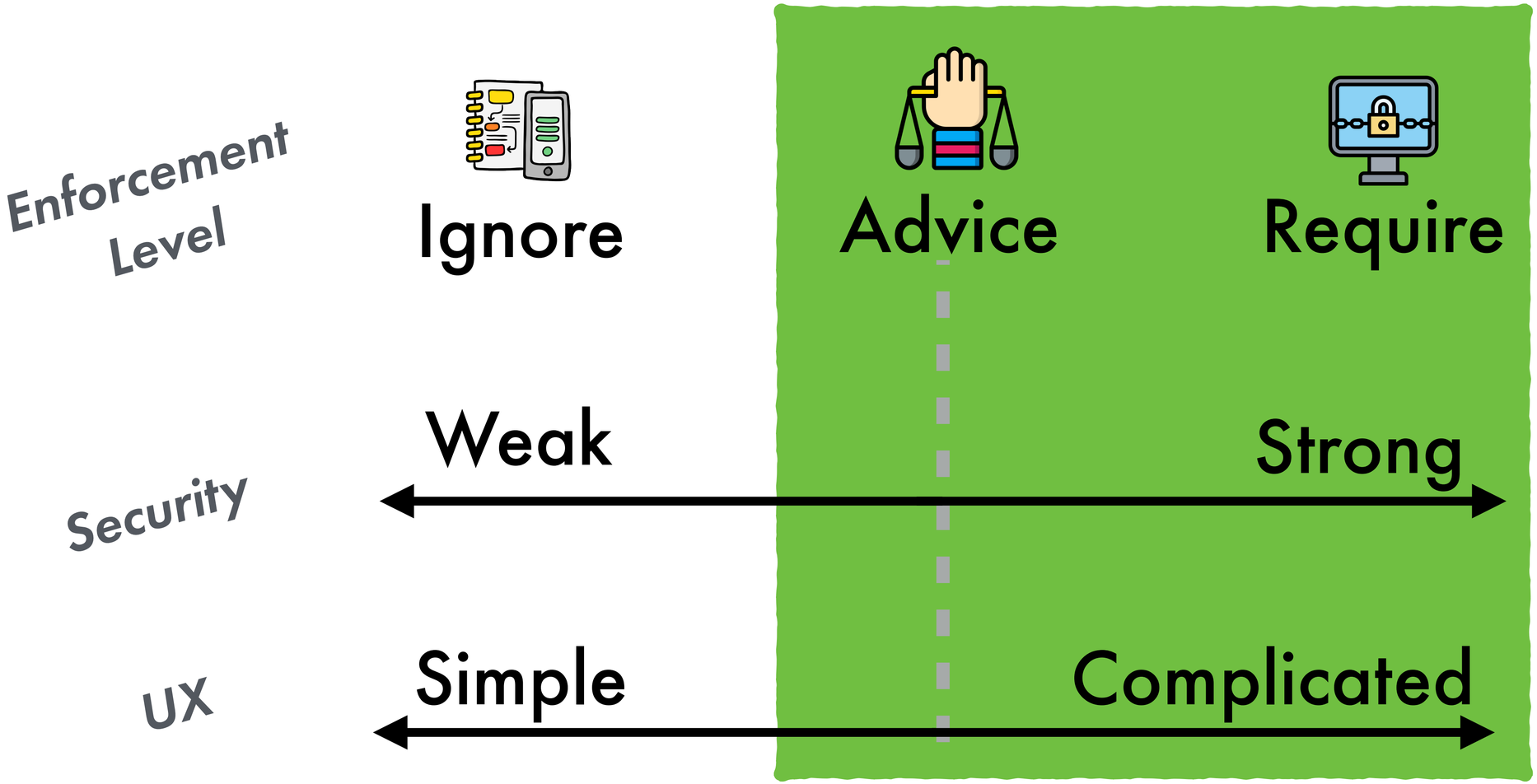
YOUR LAST LINE OF PROTECTION



a3N^g5%7*xR

123456

UX / SECURITY TRADEOFFS



#1 BUILD

Where You're Logged In

[redacted]
Chrome · **Active now**

[redacted]
Messenger · 5 hours ago

See More

Login

Change password
It's a good idea to use a strong password that you're not using elsewhere — Edit

Save your login info
On • It will only be saved on the browsers and devices you choose — Edit

Two-factor authentication

Use two-factor authentication
We'll ask for a login code if we notice an attempted login from an unrecognized device or browser. — Edit

Authorized Logins
Review a list of devices where you won't have to use a login code — View

Setting Up Extra Security

Get alerts about unrecognized logins
On • We'll let you know if anyone logs in from a device or browser you don't usually use — Edit

Choose 3 to 5 friends to contact if you get locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in — Edit

Advanced

Encrypted notification emails
Add extra security to notification emails from Facebook (only you can decrypt these emails) — Edit

See recent emails from Facebook
See a list of emails we sent you recently, including emails about security — View

#1 BUILD

Logins
Password estimation

2-factor authentication

Sessions control
Sign-in every X days

Idle time

Device/web control
Connected Devices

Web Sessions

Alerts
New sign-ins

Suspicious activity

Recovery
Recovery mail

Recovery codes

Data control
3rd party apps

Encryption method

#1 BUILD

Security

Require that all meetings are secured with one security option

Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or "Only authenticated users can join meetings". If no security option is enabled, Zoom will secure all meetings with Waiting Room. Learn more

Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Waiting Room Options

The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

- ✓ Users who are not in your account and not part of your whitelisted domains will go in the waiting room
- ✓ Host, co-hosts, and anyone who bypassed the waiting room (only if host and co-hosts are not present) can admit participants from the waiting room

Edit Options Customize Waiting Room

Require a passcode when scheduling new meetings

A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a passcode for instant meetings

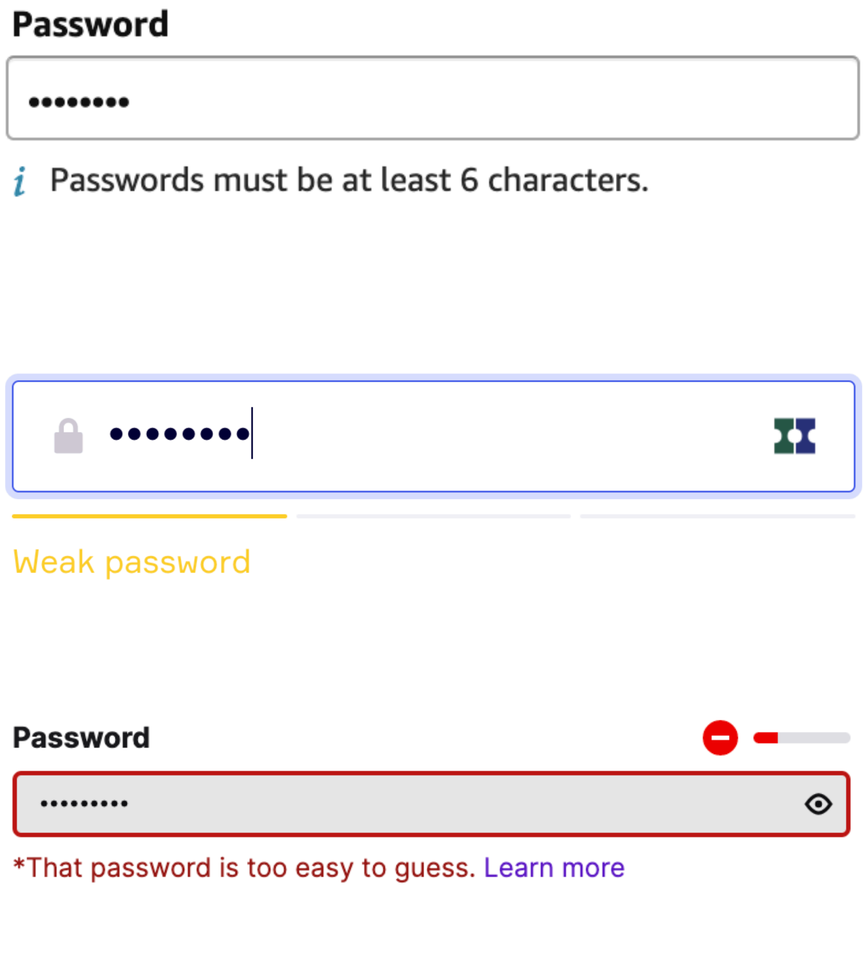
A random passcode will be generated when starting an instant meeting

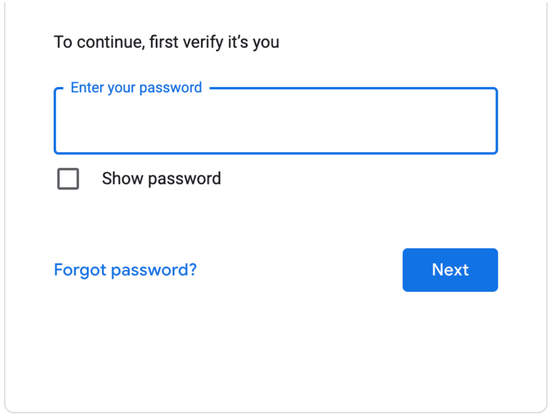
Require a passcode for Personal Meeting ID (PMI)

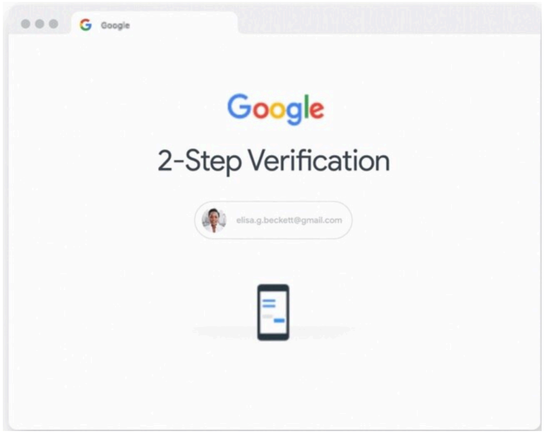
Require a passcode for Personal Audio Conference

Require passcode for participants joining by phone

#2 SET ENFORCEMENT LEVEL







#3 ENCOURAGE

Take a minute to ensure you're keeping your Dropbox account protected.
Currently reviewing your **Dropbox Dropbox.** Switch to Personal Dropbox.

1 Verify email

A current email address makes it easy to get back into your account if you ever forget your password.

Is [redacted] your current email?

Yes Contact your team admin to change your email

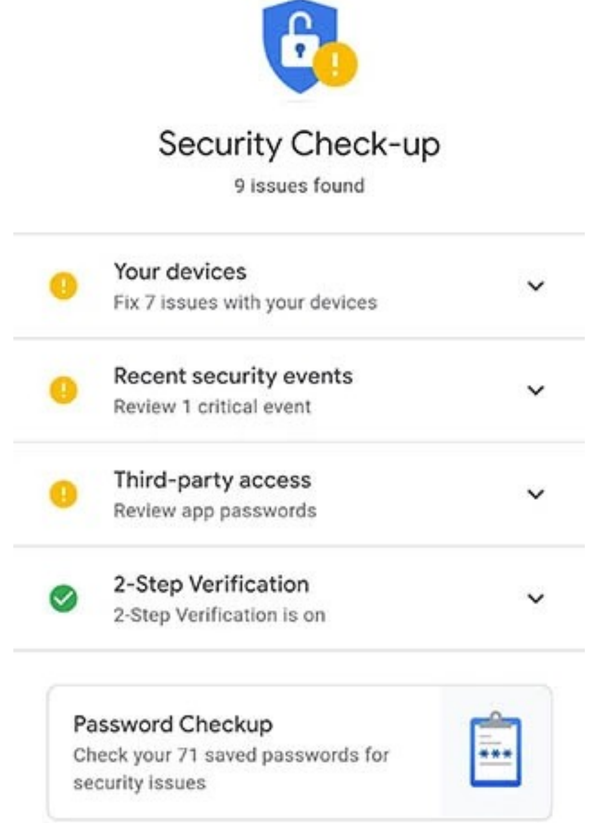
2 Review devices and browsers

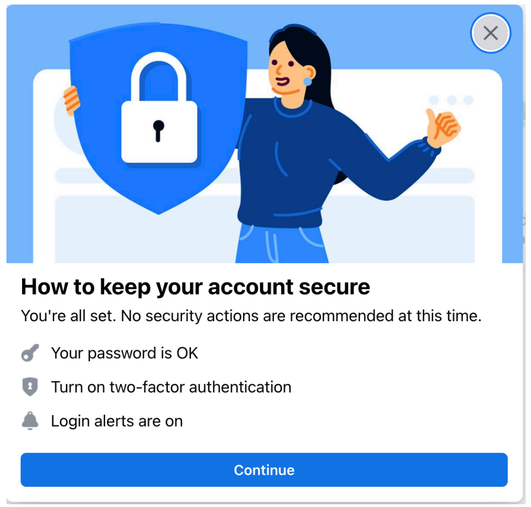
3 Review linked apps

4 Ensure your password is secure

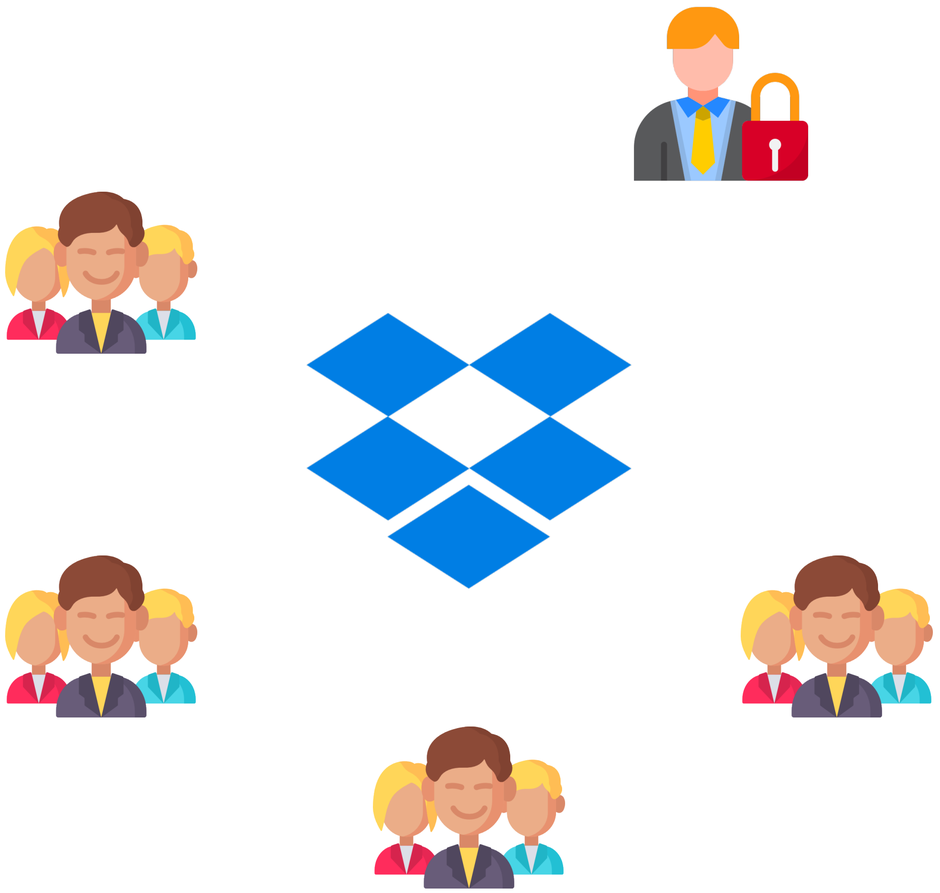
5 Review two-step verification settings

6 Try a password manager

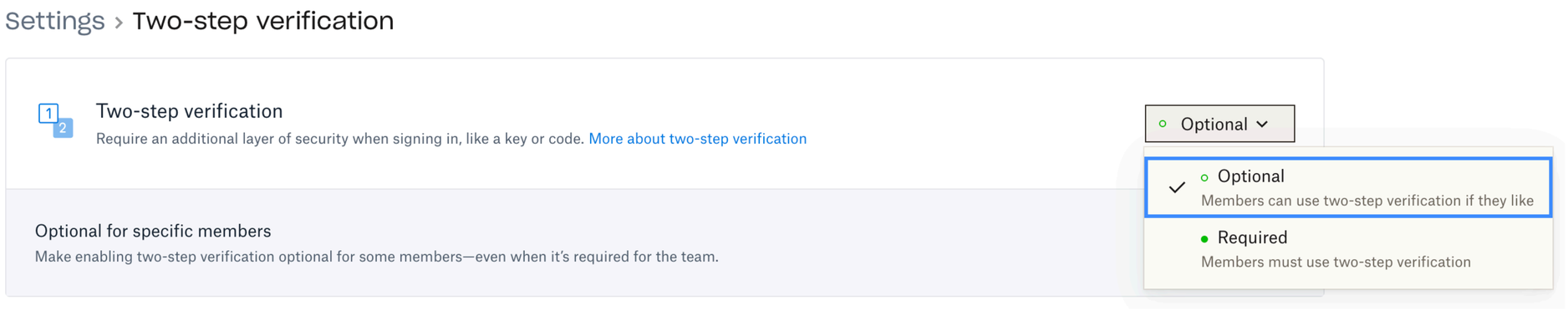




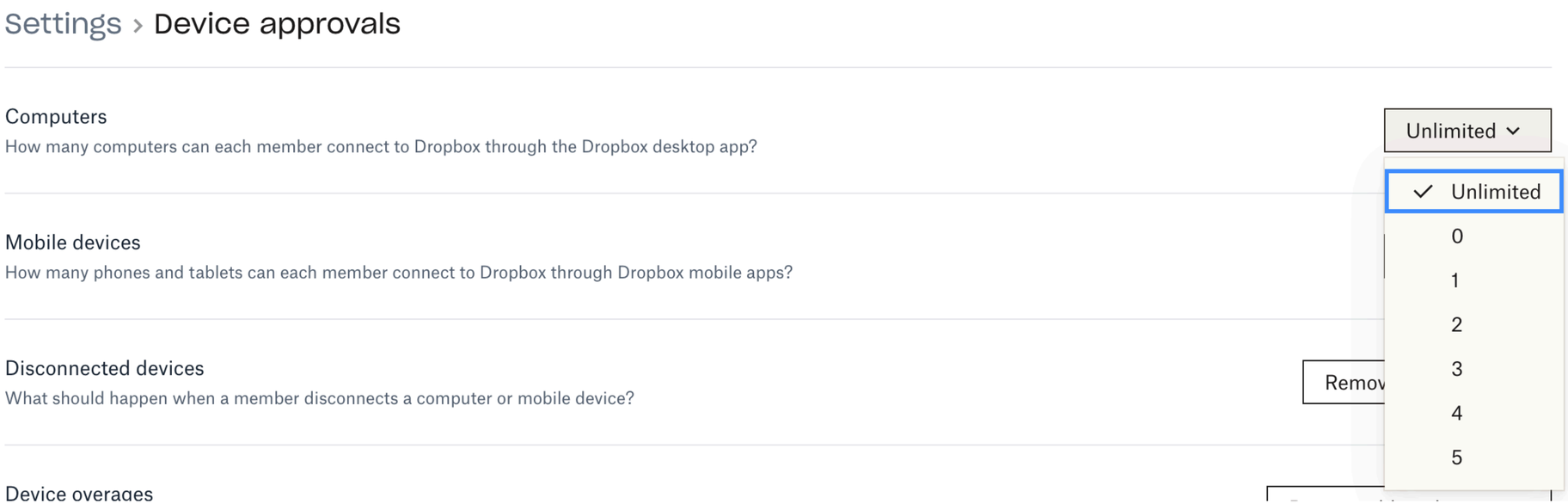
#4 DELEGATE (B2B)



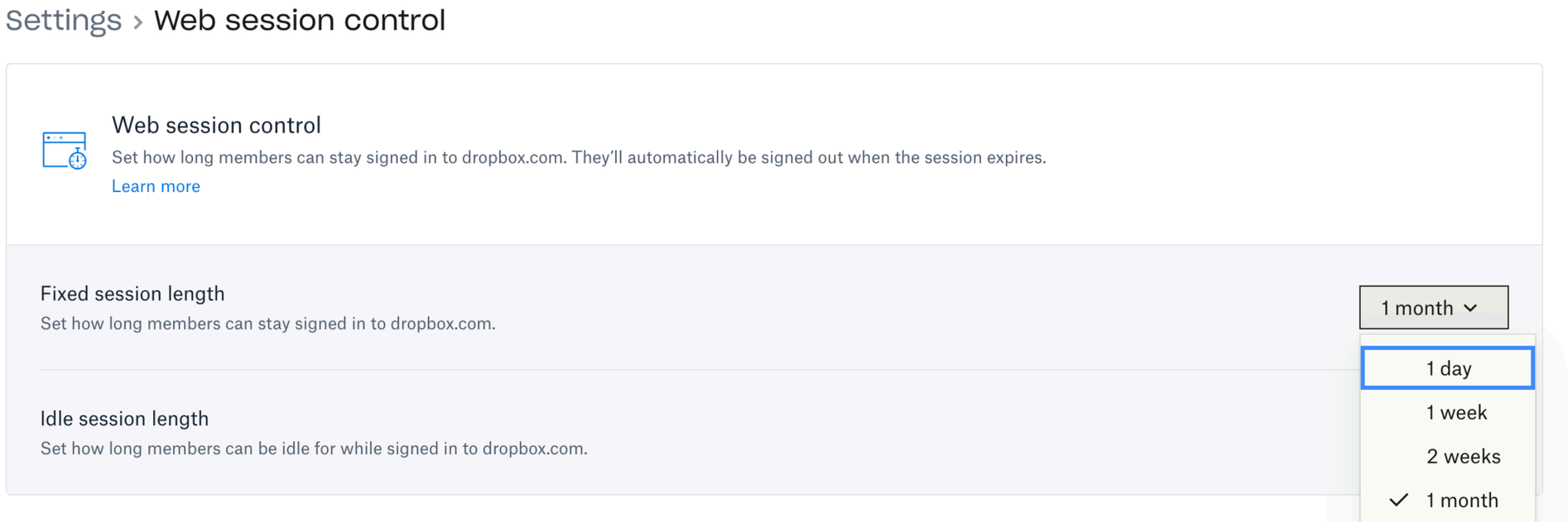
#4 DELEGATE (B2B)



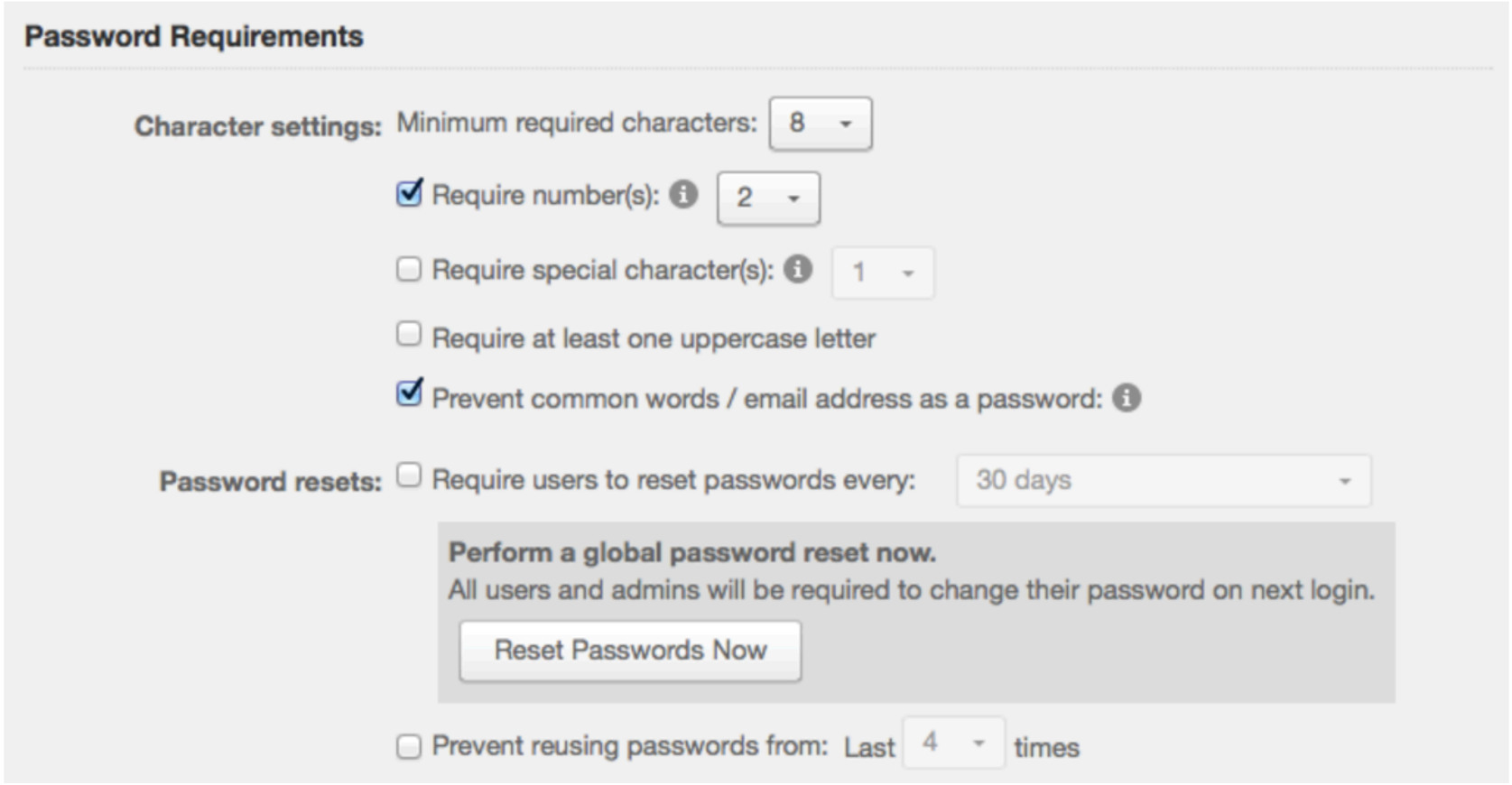
#4 DELEGATE (B2B)



#4 DELEGATE (B2B)



ADMIN CONTROL - OUR COMPETITORS



5 WHY'S

I want to have the same password controls as your competitors

Why?

I want to force my users to use long passwords with special characters, numbers, etc.

Why?

I want more control over my users' passwords

Why?

I want them to use strong passwords

Why?

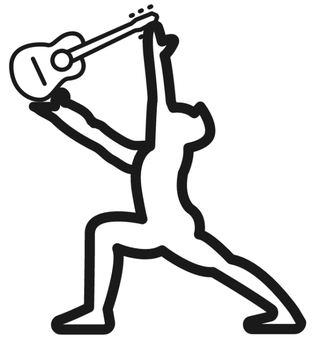
I want o reduce the risk of account hijacking

Why?

I want my team's files to be safe

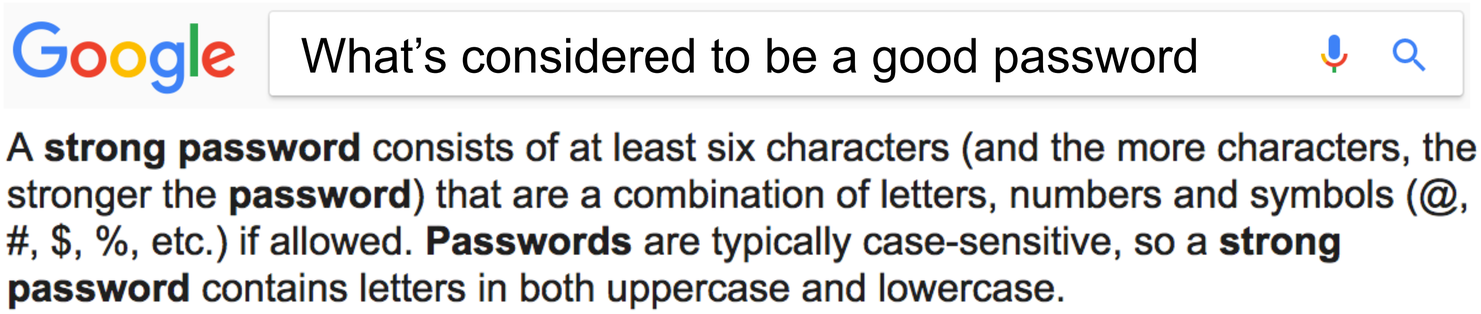
WHICH PASSWORD IS BETTER?

Tr0ub4dor&3



bluegiraffeplaysball

GOOD PASSWORD

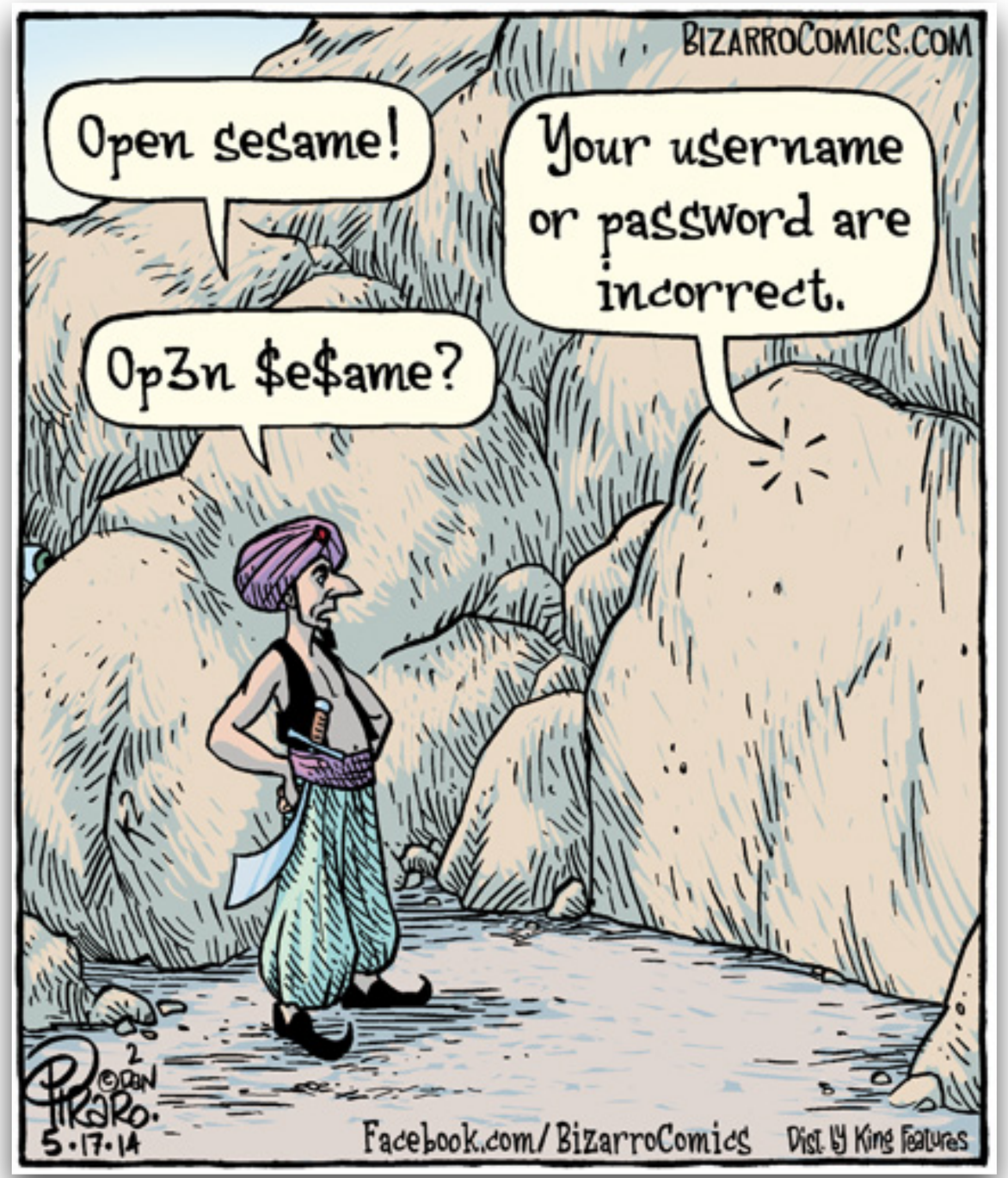


- ☑ 6+ characters
- ☑ MiXed CaSE
- ☑ numb3rs
- ☑ special ch@r@cters!

LET'S COMPARE

		
6+	👍	👍
CaSE	👍	👎
numb3rs	👍	👎
ch@r@cte	👍	👎


Alibaba
阿里巴巴


BIZARROCOMICS.COM
Open sesame!
Op3n $e$ame?
Your username or password are incorrect.
©DAN PIRARO 5·17·14
Facebook.com/BizarroComics
Dist. by King Features

Hard to guess

Easy to remember

HARD TO GUESS

of guesses required
to crack the password

NAIVE ESTIMATION

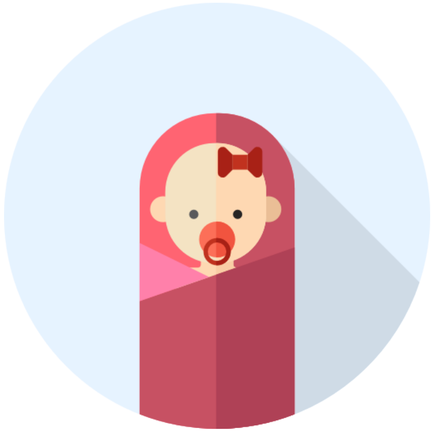
$$guesses = cardinality^{length}$$ 

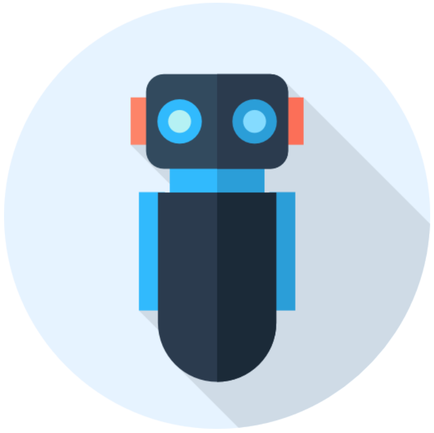
Cardinality	abc	26	→	abc+ABC+123+@$%	95
Guesses	vxcblt	26^6	→	d%ac3?	95^6
1000/sec.	⏳15 days		→	⏳140 years	

length

cardinality

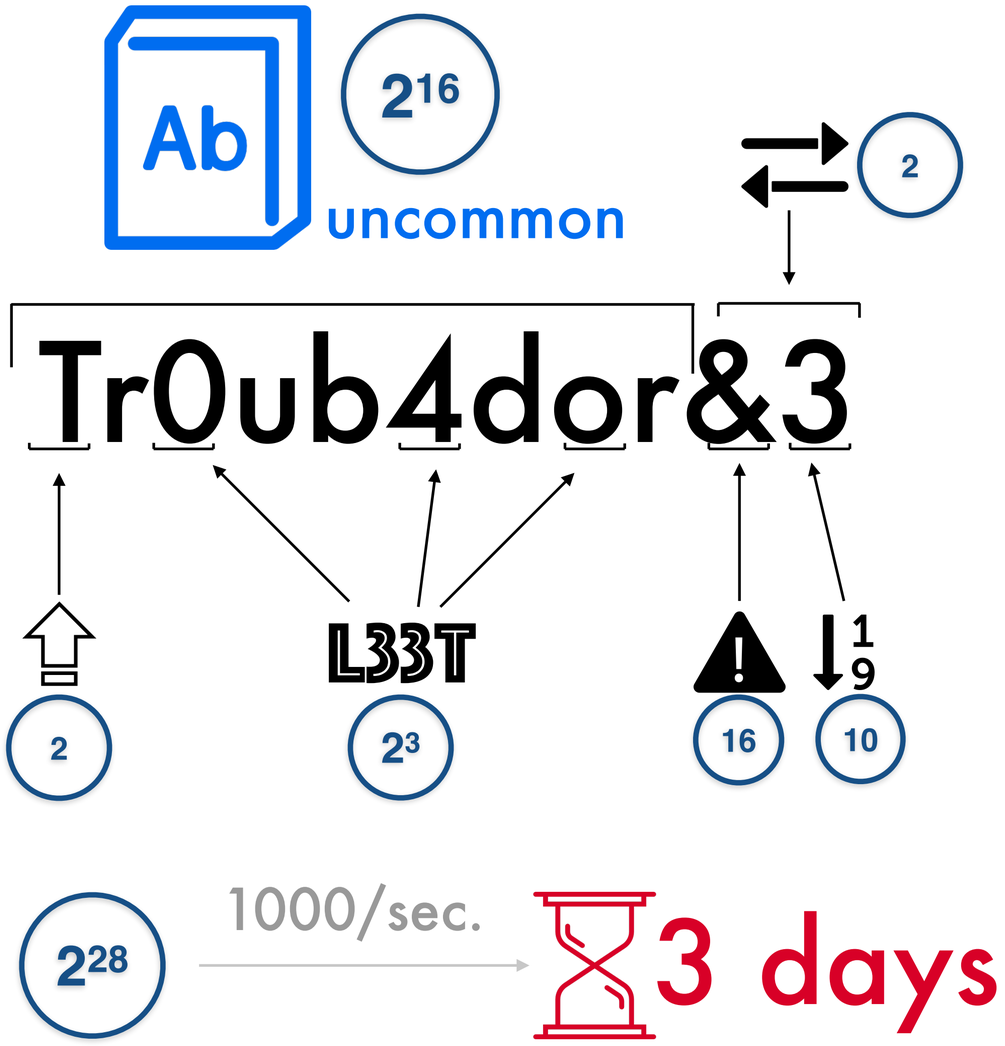
We're **humans**



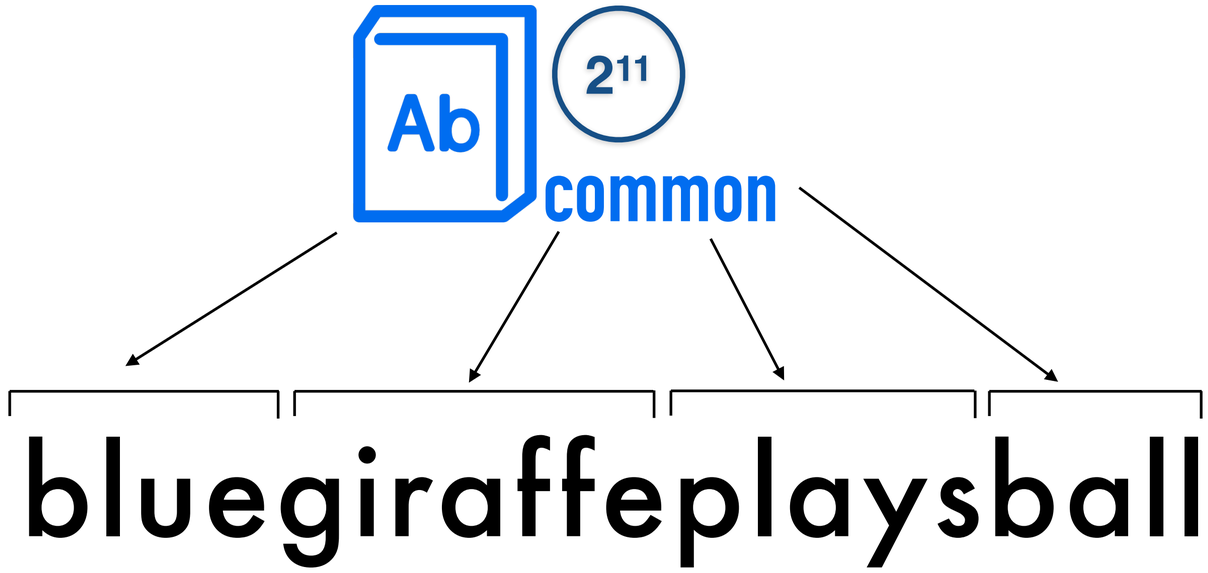


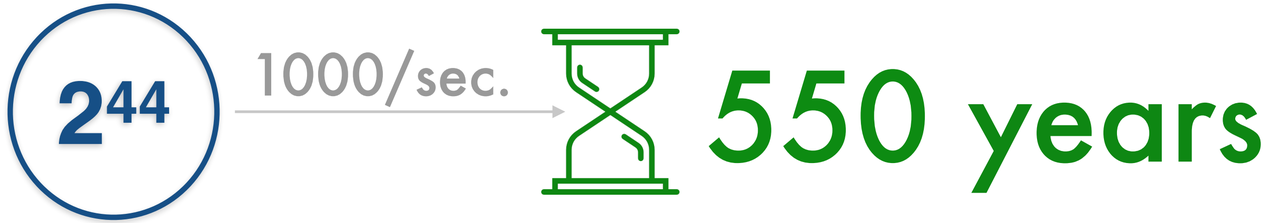
Not **robots**

HARDER TO GUESS



HARDER TO GUESS

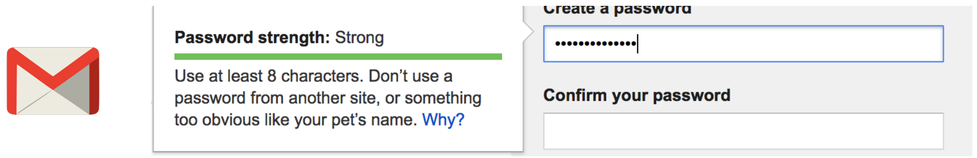


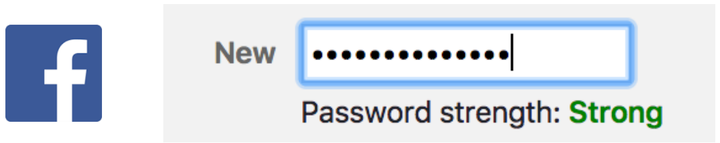


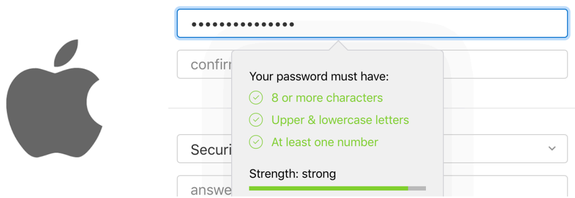
EASY TO REMEMBER

Tr0mbone?3
Troubad0r?3
Tr0ubador?3
Tr0ub4d0r!3
Tr0ubad0r?3
Tr0ub4d0r&3
:0

BIGGEST SITES ESTIMATIONS







IF WE ONLY HAD A TOOL

Password to test: password123456! Break it down!

```
Estimating strength of password "password123456!":

Approx time to crack: instant
(in seconds): 0
Strength score (1-5): 1
Entropy estimate (bits): 3
```

```
password:
  pattern: dictionary
  token: password
  rank: 1
  entropy: 0
```

```
123456:
  pattern: dictionary
  token: 123456
  rank: 2
  entropy: 1
```

```
!:
  pattern: dictionary
  token: !
  rank: 2
  l33t_entropy: 1
  entropy: 2
```

WE DO HAVE!

zxcvbn ✨

Built @ 2012 by Dan Wheeler

Open-sourced on under MIT license

10K+

HOW TO USE

```
$ npm install zxcvbn

$ node

> var zxcvbn = require('zxcvbn');

> zxcvbn('Tr0ub4dour&3');
```

FAST & LIGHT

Implemented in:

Fast: ~5-20ms for up to 25 characters

Lightweight: code:<50kb; data:<1mb;

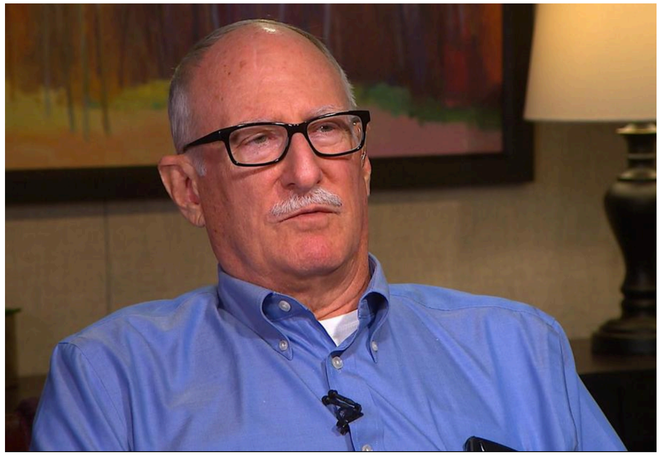
BILL BURR REGRETS

c|net REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

SECURITY

Father of passwords regrets the advice he gave

Commentary: Bill Burr thought he gave the right advice about password creation. He's decided he was wrong.



USA TODAY

NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 83° CROSSWORDS VIDEO GRATEFUL SUBSCRIBE NEWSLETTERS STOCKS M

Password expert says he was wrong: Numbers, capital letters and symbols are useless

NEWS POLITICS BORDER CRISIS TECH & MEDIA BUSINESS INTERNATIONAL THINK

SECURITY

Forget Everything You Know About Passwords, Says Man Who Made Password Rules

The Telegraph HOME | NEWS | SP

Technology Intelligence

Gadgets | Innovation | Big Tech | Start-ups | Politics of Tech | Gaming | Podcast | Te

Technology Intelligence

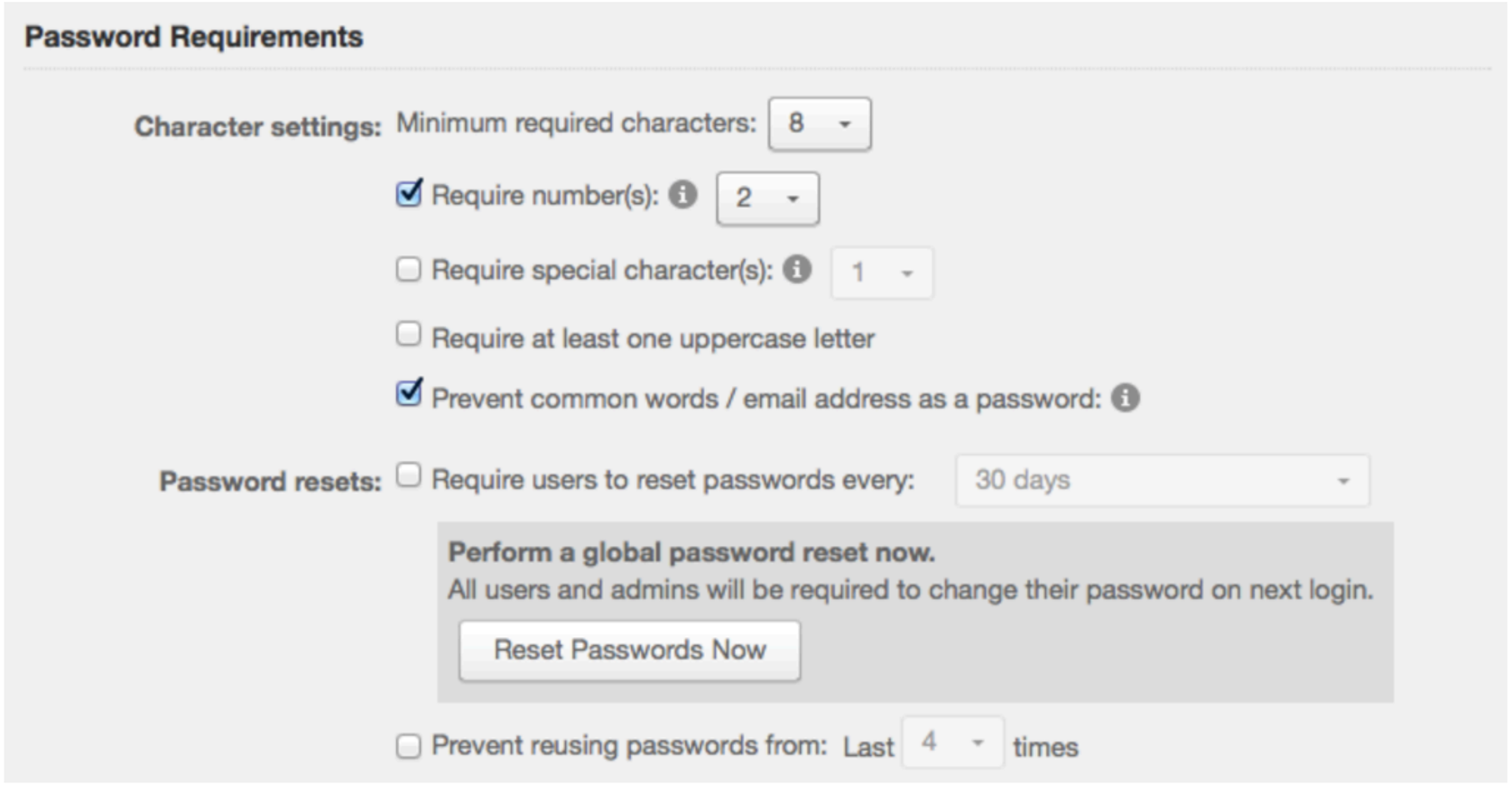
Password guru who told the world to make them complicated admits: I got it completely wrong

RECOMMENDATION UPDATE - NIST*

- ☑ No password hints
- ☑ Knowledge-based authentication (KBA) is out.
- ☑ No more expiration without reason
- ☑ No composition rules

*National Institute of Standards and Technology

ADMIN CONTROL - OUR COMPETITORS



Password strength

Require your team to set stronger passwords on their Dropbox accounts.

Strong

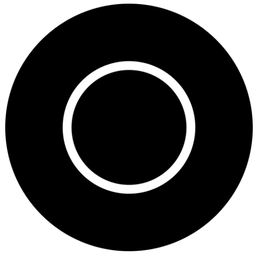
WIN, WIN, WIN

Password strength

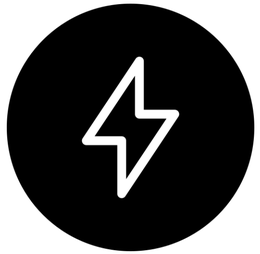
Require your team to set stronger passwords on their Dropbox accounts.

Strong

Fast



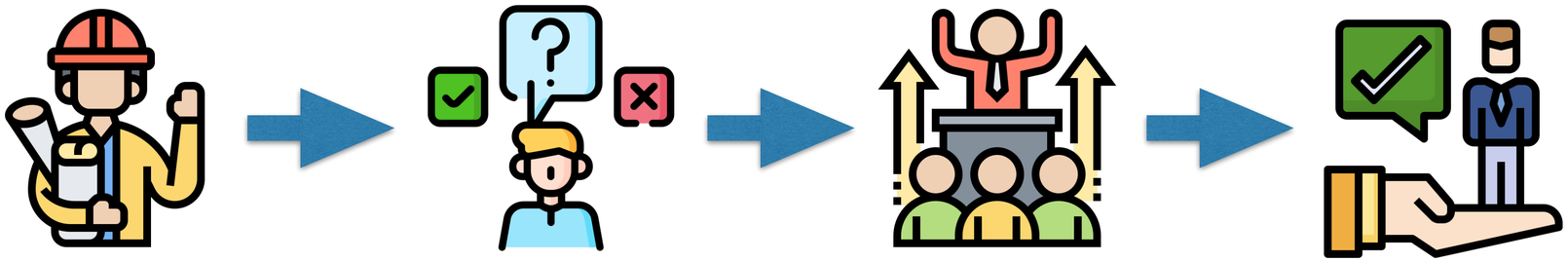
Simple



Powerful

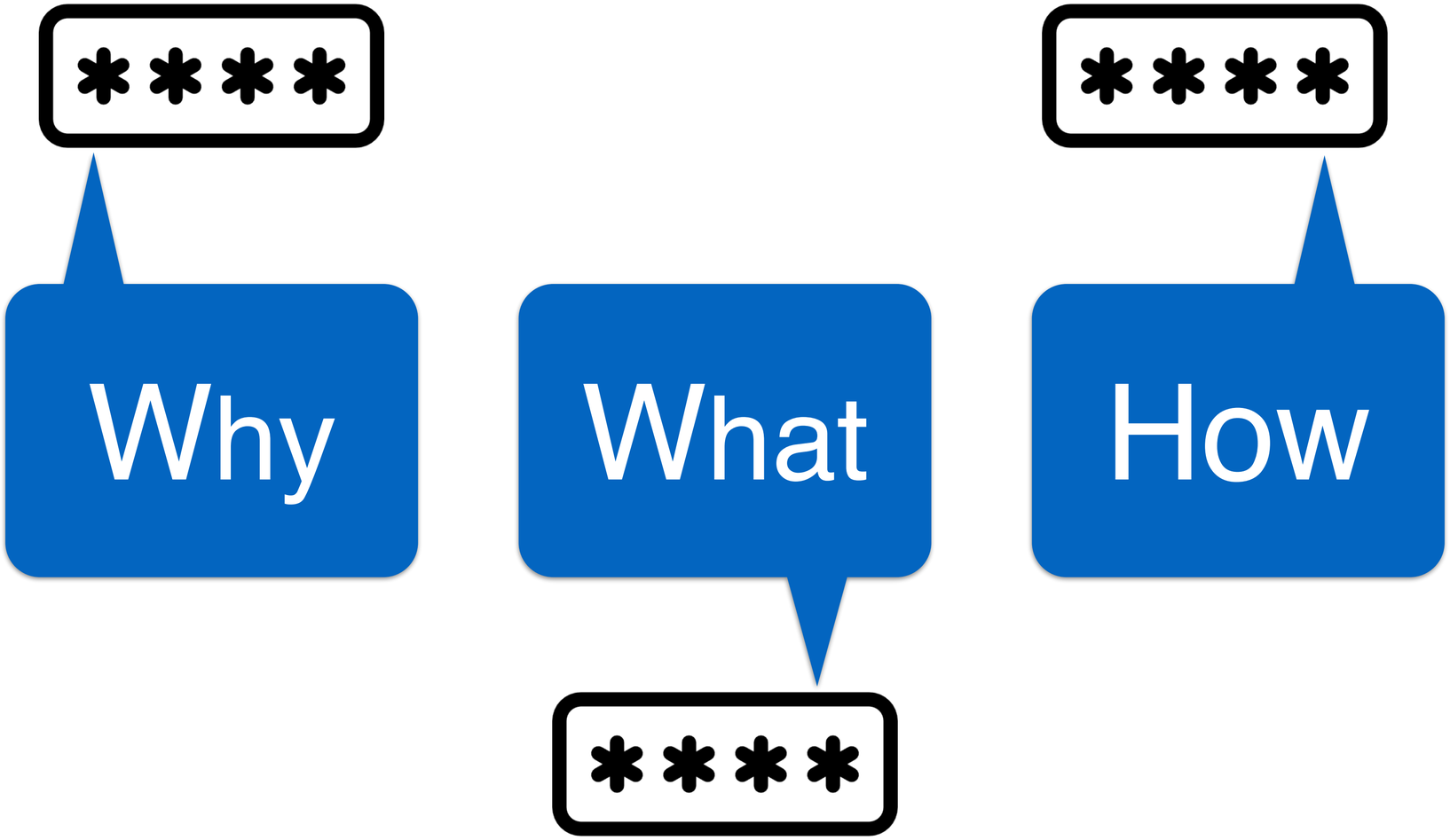
CONCLUSION

FINDING THE BALANCE



Build → Decide → Encourage → Delegate

PASSWORD ESTIMATION



SECURITY VS. UX

Don't automatically build

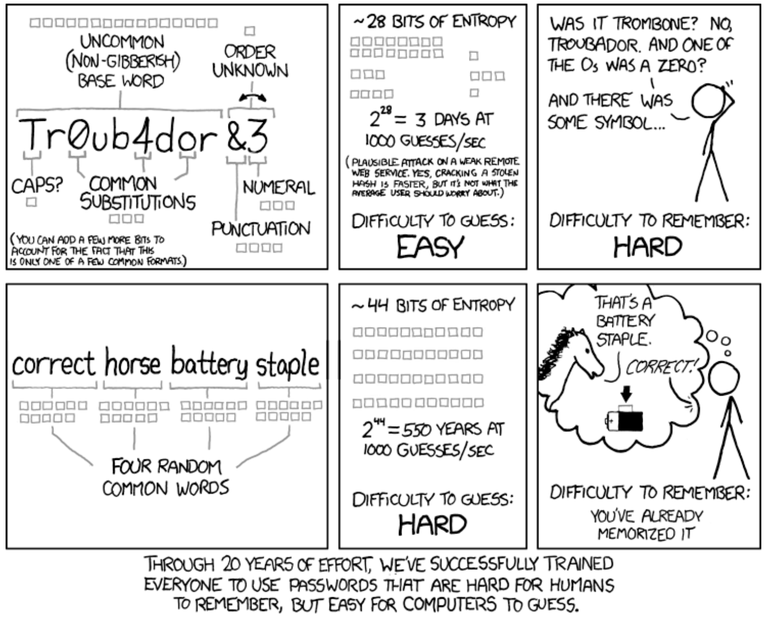
5 Whys

Smart algorithm

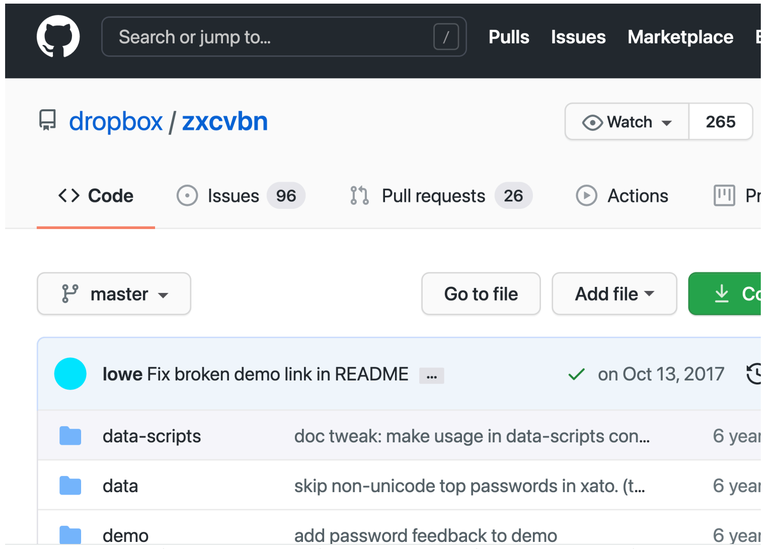
Early conversation

THANK YOU

XKCD

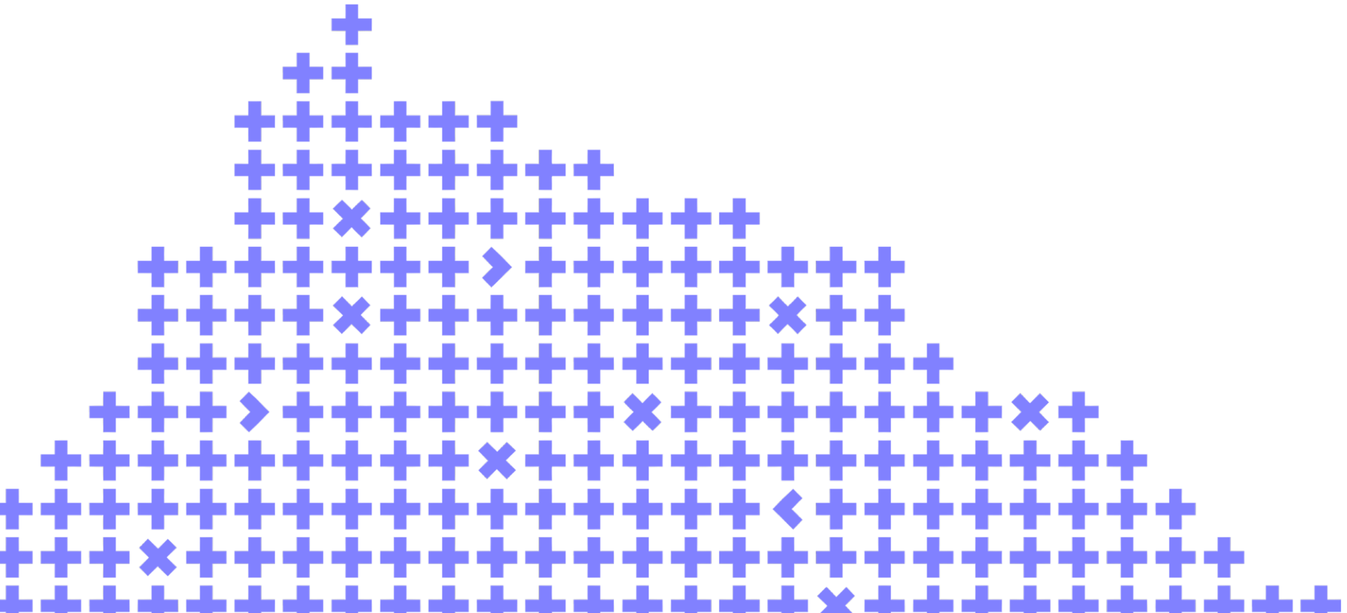


Dan Wheeler



THANK YOU

Leave your feedback! You can rate the talk and tell me what you've liked and what can be improved :)



High Load++ Armenia

Co-organizer

Yandex